

To appear in the *Journal of Mathematics and Music*
Vol. 00, No. 00, Month 20XX, 1–21

Journal of Mathematics and Music From covering to tiling modulus p
(Modulus p Vuza canons: generalities and resolution of the case
 $\{0, 1, 2^k\}$ with $p = 2$.)

Helianthe Caure^a *

^aInstitut de Recherche et Coordination Acoustique/Musique;

(v1.0 released December 2013)

Non-periodic tilings of \mathbb{Z}_N are a difficult to obtain key to a wide range of complex mathematical issues. In a musician's eyes, they are called rhythmic Vuza canons. After a short summary of the main properties of rhythmic tiling canons and after stressing the importance of Vuza canons, this article presents a new approach: modulo p Vuza canons. Working modulo p (especially with $p = 2$) allows Vuza canons to be computed very quickly. But going back to traditional Vuza canons requires understanding of when and how the tiling is a covering. The article's main result is a complete case construction of a modulo 2 tiling. This first solution of a modulo 2 tiling is proved in a constructive way, which, it is hoped, is expandable to every modulo p tiling. Following this path may lead to a solution to the problem of building modulo p tilings and thus a solution to the problem of easily finding traditional Vuza canons.

Keywords: translational tiling, rhythmic canons, Vuza, finite field polynomials, multiset

1. Introduction

1.1. Context

The science of rhythmic tiling canons came into being thanks to both Dan Tudor Vuza (1991-1993), who approached the subject from a musical point of view, and György Hajós (1949), who previously developed a mathematical theory -the notion of finite abelian group factorization (while he was solving the Minkowski conjecture)- that was later linked to Vuza's work by Moreno Andreatta (1996).

Musically, a rhythmic tiling canon is a canon where only the onsets matter. A musical note is usually described by its pitch, onset, offset, velocity... The canon is said rhythmic because most of the note classical attributes are not relevant: it is a canon where the main voice is a pattern of onsets. The tiling property of the canon comes from the constraint that the pattern of onsets and its translates -the other voices of the canon- must tile the time axis: one must hear at every beat one and only one onset.

Thanks to Vuza's modelisation of rhythm (Vuza 1985), such a canon is equivalent to a tiling of the discrete line \mathbb{Z} by a finite integers set and its translates. This, as we will explain later, can be represented by a direct sum of a two integers sets being equal to \mathbb{Z} .

Lagarias and Wang have proved in a more general case (Lagarias and Wang 1996, theorem 5) that a tiling of the line by translations is periodic. This result was already known by Hajós and DeBruijn (Hajós 1949), although they never proved it in details.

*Corresponding author. Email: Helianthe.Caure@ircam.fr

Hence, for modelling rhythmic tiling canons, we will not focus on a tiling of \mathbb{Z} by a finite set of integers, but on a tiling of \mathbb{Z}_N .

For a more complete history of rhythmic canons and recent research on the topic, the reader is invited to refer to the special issues on the topic which appeared in both Journal of Mathematics & Music (2009) and Perspectives of New Music (2011).

1.2. Model

DEFINITION 1.1 We will denote equivalently a rhythmic pattern by

- (1) a finite set A of non negative integers containing 0
- (2) a polynomial $A(X) \in \{0, 1\}[X]$
- (3) an infinite word with finitely many non-zero letters or a finite word A_{0-1} over the alphabet $\{0, 1\}$.

By denoting for any word u , the subword of length k starting at the n -th letter $u[n, \dots, n+k-1] \forall k \in \mathbb{N}^*$, the equivalent notations are linked by

$A(X) = \sum_{a \in A} X^a$ and $\forall n \in \mathbb{N} \ A_{0-1}[n] = \mathbb{1}_A(n)$, where $\mathbb{1}_A$ is the characteristic function of A and its length verifies $\max A + 1 \leq |A_{0-1}| \leq \infty$.

Elements of a rhythmic pattern are called onsets.

DEFINITION 1.2 Let $*$ be a standard set-theoretic operation (like the sum or cartesian product) between sets of integers, and $N \in \mathbb{N}$. We note $*_N$ the operation defined by $A *_N B = \{a *_N b \bmod N, a \in A, b \in B\}$.

DEFINITION 1.3 Let $N \in \mathbb{N}^*$, the rhythmic pattern A tiles \mathbb{Z}_N if there exists another rhythmic pattern B such that one of the following equivalent conditions is satisfied:

- (1) $A \oplus_N B = \mathbb{Z}_N$ where \oplus is the direct sum (or injective sum $\oplus : A \times B \rightarrow \mathbb{Z}$)
- (2) $A(X) \cdot B(X) = 1 + X + \dots + X^{N-1} \bmod (X^N - 1)$
- (3) $\mathbb{1}_A \star \mathbb{1}_B = \mathbb{1}_{\mathbb{Z}_N}$ where \star is the convolution product.

We say that (A, B) is a rhythmic tiling canon (RTC) of \mathbb{Z}_N , or that the pattern A tiles \mathbb{Z}_N with the (pattern of) entries B .

Remark 1.4 It is important to understand that a rhythmic pattern A that tiles \mathbb{Z}_N doesn't have to be included in $\{0, \dots, N-1\}$. Indeed, it is possible that there exists $a \in A$ such that $N < a$, because only the elements of the sum $A + B$ are projected in \mathbb{Z}_N . The reader can even prove that from a RTC (A, B) of \mathbb{Z}_N , one can build A' verifying this latter condition such that (A', B) is a RTC of \mathbb{Z}_N .

Example 1.5 A rhythmic pattern can be written in the following ways

- (1) $A = \{0, 1, 4, 5\}$
- (2) $A(X) = 1 + X + X^4 + X^5$
- (3) $A_{0-1} = 110011$ or $A_{0-1} = 1100110000$ or $A_{0-1} = 1100110\dots$

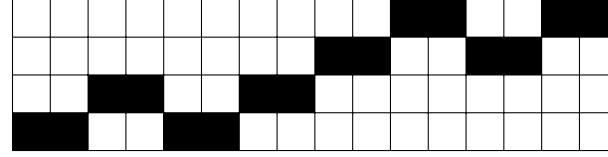
It tiles \mathbb{Z}_{16} with $B = \{0, 2, 8, 10\}$.

Remark 1.6 From now on, instead of writing n times a letter a , we will denote $\bar{a}^n = aa \dots a$.

An easy way to represent a RTC (A, B) , which helps “seeing” the rhythm, is on a grid with its x-axis corresponding to the time, and its y-axis the entrance of new voices from B playing the pattern A . An onset of a note $a + b \in A \oplus_N B$ of the RTC is depicted by

a black square in position $(a + b \bmod N, i)$, with $B[i] = b$.

Example 1.7 One can represent the RTC $(\{0, 1, 4, 5\}, \{0, 2, 8, 10\})$ of \mathbb{Z}_{16} in the following way:



(0,0)

DEFINITION 1.8 A RTC (A, B) is compact if $A \oplus_N B = A \oplus B = \llbracket 0, N - 1 \rrbracket$ exactly, without need of projection in \mathbb{Z}_N .

Example 1.9 $(\{0, 1, 4, 5\}, \{0, 2\})$ is compact, whereas $(\{0, 1, 3, 6\}, \{0, 4\})$ is not.

DEFINITION 1.10 Let $k \in \mathbb{N}^*$, and A be a rhythmic pattern which tiles \mathbb{Z}_N . We note $\bar{A}^k = A \oplus \{0, N, 2N, \dots, (k-1)N\}$ its k -concatenation.

As shown by Amiot (2005) some transformations of RTC give other RTC, see:

PROPOSITION 1.11 (Duality) (A, B) is a RTC of \mathbb{Z}_N iff (B, A) is a RTC of \mathbb{Z}_N

PROPOSITION 1.12 (Concatenation) Let $k \in \mathbb{N}^*$, (A, B) is a RTC of \mathbb{Z}_N iff (\bar{A}^k, B) is a RTC of \mathbb{Z}_{kN} .

Example 1.13 The dual of the canon depicted on example 1.7 is the 2-concatenation of the dual of the first canon of example 1.9.

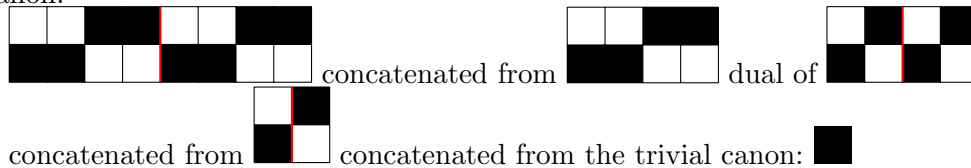
1.3. Vuza Canons

DEFINITION 1.14 A RTC (A, B) of \mathbb{Z}_N is periodic if there exists $0 < k < N$ such that $A +_N \{k\} = A$ or $B +_N \{k\} = B$.

If a canon is not periodic, it is called a Vuza canon (VC).

THEOREM 1.15 (Amiot (2005)) Every RTC can be deduced by concatenation and duality transformations from VC and the trivial canon $(\{0\}, \{0\})$.

Example 1.16 $\{0, 1, 4, 5\} \oplus \{0, 2\} = \mathbb{Z}_8$ is concatenated from $\{0, 1\} \oplus \{0, 2\} = \mathbb{Z}_4$, whose dual is concatenated from the dual of $\{0, 1\} \oplus \{0\} = \mathbb{Z}_2$, concatenated from the trivial canon.



Remark 1.17 It means that VC are the basis of RTC under concatenation operation. Thus, if one manages to obtain every VC, one has a constructive way to get every RTC. Note that in practice, it is difficult to build RTC from VC, even if we know that they exist and the size of their tile:

THEOREM 1.18 *There exist VC of \mathbb{Z}_N for, and only for N not of the form:*

$$N = p^\alpha, N = p^\alpha q, N = p^2 q^2, N = pqr, N = p^2 qr, N = pqrs$$

with p, q, r, s distinct primes.

Proof. This full result has been shown step by step by Hajós (1949), Rédei (1950), De Bruijn (1953), Sands (1957) and later by Vuza (1985) independently. ■

Those non-periodic canons are also the key to understanding whether a given rhythmic pattern tiles or not:

The tiling condition

$$A(X) \cdot B(X) = 1 + X + \dots + X^{N-1} = \frac{X^N - 1}{X - 1} \bmod (X^N - 1)$$

gives the idea of splitting the N -th roots of unity between the factors A and B , hence, looking for their cyclotomic factors.

DEFINITION 1.19 *Let A be a rhythmic pattern, we note*

$$R_A = \{d \in \mathbb{N}^*, \text{ the } d\text{-th cyclotomic polynomial divides } A(X)\},$$

$$S_A = \{p^a \in R_A, p \text{ prime}, a \in \mathbb{N}^*\}.$$

DEFINITION 1.20 *Let A be a rhythmic pattern, the following three conditions are called Coven-Meyerowitz conditions:*

(T_0) : A tiles

(T_1) : $A(1) = \prod_{p^\alpha \in S_A} p$

(T_2) : If $p_1^\alpha, p_2^\beta, \dots, p_r^\gamma \in S_A$ then $p_1^\alpha \cdot p_2^\beta \cdot \dots \cdot p_r^\gamma \in R_A$ with p_i distinct primes.

They were introduced by Coven and Meyerowitz (1999) in the currently best attempt to get a necessary and sufficient condition to know if whether a rhythmic pattern can tile or not.

THEOREM 1.21 (Coven and Meyerowitz (1999))

(1) (T_0) \Rightarrow (T_1)

(2) (T_1) \wedge (T_2) \Rightarrow (T_0)

(3) If $\sharp A$ has at most two prime factors, then (T_0) \Rightarrow (T_1) \wedge (T_2)

PROPOSITION 1.22 (Amiot (2005)) *Condition (T_2) is closed under duality and concatenation transformations.*

COROLLARY 1.23 *We have (T_0) \Rightarrow (T_2) for every RTC iff (T_0) \Rightarrow (T_2) for every VC.*

Remark 1.24 This corollary emphasises the importance of VC. Those non-periodic canons are nonetheless the construction basis of any RTC, but they are also the bottom line to understand if a given rhythmic canon would tile.

Though, enumeration of VC is still out of reach of mathematicians: the best we currently have is an exploration algorithm to obtain slowly all the VC with a given period. It was improved recently by Kolountzakis and Matolcsi (2009), but it is still exponential.

The next section endeavours to look at VC in a more complex space, which makes them easier to obtain, with a still distant hope of going back to VC of \mathbb{Z}_N in a non-exponential way.

2. Modulus p tiling

Many RTC properties are formulated in polynomial notation (like 1.21), and the ring $\mathbb{Z}[X]/(X^N - 1)$ seems fitted for their study. However, this ring is not factorial, hence, one cannot use the decomposition in irreducible elements of the complete polynomial $1 + X + \dots + X^{N-1}$ to obtain all the factors in $\{0, 1\}[X]$.

The polynomial notation of the tiling condition (2nd point or 1.3) gives the idea, introduced in (Amiot 2004) to work in the set $\{0, 1\}[X]$ of polynomials with coefficients 0 or 1, but it is not a ring. Thus, we try to work in the ring $\mathbb{F}_2[X]$ so that we have

$$\begin{aligned} \mathbb{F}_2[X] \times \mathbb{F}_2[X] &\longrightarrow \mathbb{F}_2[X] \\ (A, B) &\longmapsto A \cdot B \end{aligned}$$

and the tiling condition becomes the divisibility of $1 + X + \dots + X^{N-1}$ by $A(X) \bmod (X^N - 1, 2)$, i.e. the classic divisibility condition in $\mathbb{Z}[X]/(X^N - 1, 2) = \mathbb{F}_2[X]/(X^N - 1)$, where $(X^N - 1, 2)$ denotes the ideal generated by the set $\{2, X^N - 1\} \subset \mathbb{Z}[X]$.

We then extend the idea to the ring $\mathbb{F}_p[X]$, p prime, and we obtain the notion of tiling modulo p .

DEFINITION 2.1 (A, B) is a RTC of \mathbb{Z}_N modulo p if

$$A(X) \cdot B(X) = 1 + X + \dots + X^{N-1} \bmod (X^N - 1, p).$$

Modulo p tiling is relevant from a mathematical point of view, but also musically, because it enriches RTC with harmony, allowing notes superposition. From now, we will denote RT_pC for a modulo p RTC.

Remark 2.2 The equivalent notations with sets from RTC are adaptable with multisets to RT_pC :

Let A and B two rhythmic patterns, (A, B) is a RT_pC of \mathbb{Z}_N if the multiset $C = A +_N B = \{a + b \bmod N, a \in A, b \in B\}$ verifies $\mathbb{1}_C(n) \equiv 1 \bmod p$ if $n \in \{0, \dots, N-1\}$, and $\mathbb{1}_C(n) = 0$ elsewhere, with $\mathbb{1}_C$ being the multiset characteristic function.

Remark 2.3 When we consider a finite multiset C , we can also adapt the notation C_{0-1} to RT_pC :

Let C be a finite multiset of non-negative integers, we note C_{0-p} the infinite word with finitely many non-zero letters or the finite word, over the alphabet $\{0, \dots, p-1\}$, verifying $\forall n \in \mathbb{N}, C_{0-p}[n] = \mathbb{1}_C(n) \bmod p$ and $\max C + 1 \leq |C_{0-p}| \leq \infty$.

To avoid the confusion between the classical notation C_{0-1} and C_{0-2} for a RT_2C , we do not use the notation $C_{0-(p-1)}$ for this multiset, even if it seems more fitting.

Example 2.4 $(\{0, 1, 3\}, \{0, 2, 3\})$ is a RT_2C of \mathbb{Z}_7 :

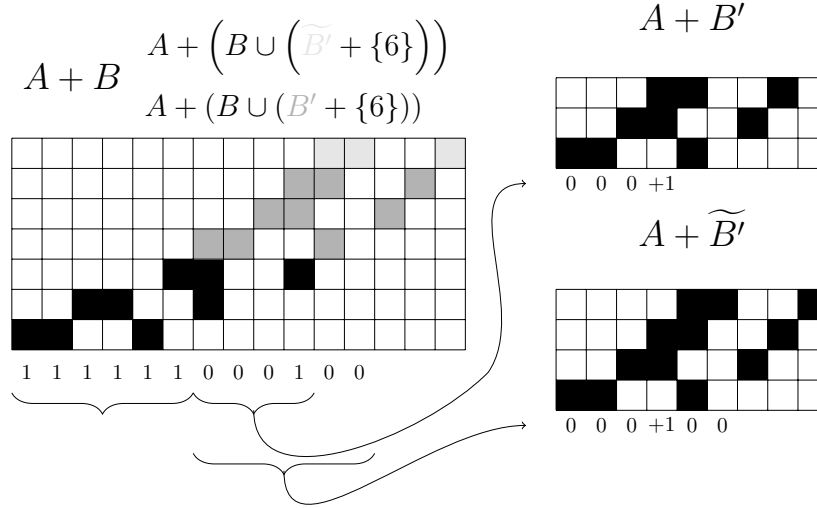
$$(1) \ A +_7 B = \{0, 1, 2, 3, 3, 3, 4, 5, 6\}$$

give the same under-cover: $UC_p(i)_1 = UC_p(i)_2$, we will need the same B' to fill it. But the minimal size of an under-cover depends on both A and B .

Example 2.13 Let $A = \{0, 1, 4\}$ and $B = \{0, 2, 5\}$. We have $A + B = \{0, 1, 2, 3, 4, 5, 6, 6, 9\}$, hence $(A + B)_{0-2} = 1111110001 (= 1111112001)$ and an under-cover starting at index 6 is $UC_2(6) = 0001$. We can fill this under-cover with $B' = \{0, 2, 3\}$.

Indeed, we have $A + (B \cup (B' + \{6\})) = \{0, 1, 2, 3, 4, 5, 6, 6, 6, 7, 8, 9, 9, 9, 10, 10, 12, 13\}$, thus $(A + (B \cup (B' + \{6\})))_{0-2} [6, 9] = 1111$.

Note that if we had chosen a longer under-cover, see $\widetilde{UC}_2(6) = 000100$, it would have been filled with $\widetilde{B}' = \{0, 2, 3, 4\}$ and not B' , because $(A + (B \cup (\widetilde{B}' + \{6\})))_{0-2} [6, 11] = 111111$ and $(A + (B \cup (B' + \{6\})))_{0-2} [6, 11] = 111100 \neq \widetilde{1}^6$.



Remark 2.14 When one wants to tile with a pattern A , one can imagine filling the null under-cover $\overline{0}^k$ for some $k \in \mathbb{N}$, starting at index 0.

This is the meaning of an under-cover: it can be seen as a partial covering that one needs to fill to obtain a tiling. This is how the greedy algorithm presented below works.

DEFINITION 2.15 *If one fills an under-cover $UC_p(i)$ of (A, B) with B' , then we call “following under-cover” an under-cover of $(A, B \cup (B' + \{i\}))$, starting at index $i + |UC_p(i)|$. It will be denoted UC'_p .*

Example 2.16 In the previous example 2.13, a following under-cover of $UC_2(6)$ is $UC'_2(10) = 0011$.

DEFINITION 2.17 (A, B) is a compact $RT_p C$ of \mathbb{Z}_N if

$$A(X) \cdot B(X) = 1 + X + \dots + X^{N-1} \mod p.$$

THEOREM 2.18 (Warusfel 1971) *Let p prime and $P \in \mathbb{F}_p[X]$ such that $P(0) \neq 0$, then there exists $N \in \mathbb{N}$ such that P divides $X^N - 1$.*

Remark 2.19 As first noticed by Amiot (2005), this theorem entails that any rhythmic

pattern tiles modulo p :

Let $A(X) \in \mathbb{Z}[X]$ be a rhythmic pattern and a fixed p prime. Considering the polynomial $P(X) = A(X)(X - 1) \in \mathbb{F}_p[X]$, and the quotient polynomial $Q \in \mathbb{F}_p[X]$ given by the theorem such that $P(X) \cdot Q(X) = (X^N - 1) \bmod p$ we can obtain the tiling condition $P(X) \cdot \tilde{Q}(X) = (X^N - 1) \bmod (X^N - 1, p)$ with \tilde{Q} a polynomial representing a rhythmic pattern. Indeed, by iterating the transformation

$$\alpha X^k = (\alpha - 1)X^k + X^{k+N} \bmod (X^N - 1)$$

over the polynomial Q , it can be associated to a rhythmic pattern $\tilde{Q} \in \mathbb{Z}[X]$, i.e. a polynomial of $\{0, 1\}[X]$.

Note that in $\mathbb{F}_2[X]$, every polynomial has its coefficients in $\{0, 1\}$ which means that this transformation is unnecessary, hence every rhythmic pattern gives a compact RT_2C . Indeed, it is clear that the non-compactness of a RTC (in \mathbb{Z} or \mathbb{F}_p) comes from the projection modulo $(X^N - 1)$; i.e. here from the transformation we apply on Q .

Example 2.20 In $\mathbb{F}_3[X]$, let $A(X) = 1 + X + X^3$ be a rhythmic pattern. It verifies

$$\begin{aligned} X^{24} - 1 &= A(X)(X - 1) \cdot (X^{20} + X^{19} + 2X^{17} + 2X^{15} + 2X^{14} + 2X^{13} \\ &\quad + 2X^{10} + X^9 + 2X^8 + X^7 + X^6 + X^5 + 2X^4 + 2X^3 + X^2 + 1) \end{aligned}$$

The quotient polynomial $Q(X) = X^{20} + X^{19} + 2X^{17} + 2X^{15} + 2X^{14} + 2X^{13} + 2X^{10} + X^9 + 2X^8 + X^7 + X^6 + X^5 + 2X^4 + 2X^3 + X^2 + 1$ does not have its coefficients in $\{0, 1\}$, thus is not a rhythmic pattern. By applying the transformation $2X^k = X^k + X^{k+24}$ to its terms ($2 * X^{17}, 2 * X^{15}, 2 * X^{14}, 2 * X^{13}, 2 * X^{10}, 2 * X^8, 2 * X^4, 2 * X^3$), we obtain the polynomial

$$\begin{aligned} \tilde{Q}(X) &= X^{20} + X^{19} + X^{41} + X^{17} + X^{39} + X^{15} + X^{38} + X^{14} + X^{37} \\ &\quad + X^{13} + X^{34} + X^{10} + X^9 + X^{32} + X^8 + X^7 + X^6 + X^5 + X^{28} \\ &\quad + X^4 + X^{27} + X^3 + X^2 + 1 \end{aligned}$$

which is a rhythmic pattern verifying

$$A(X) \cdot \tilde{Q}(X) = 1 + X + \dots + X^{23} \bmod (X^{24} - 1, 3).$$

This theorem has inspired a modulo p tiling algorithm in (Amiot 2011). We present here an algorithm devised from the previous one, but improved inasmuch as it is greedy and optimal for any rhythmic pattern which gives a compact RT_pC , a fortiori for any rhythmic pattern with $p = 2$ thanks to remark 2.19.

Require: $A \subset \mathbb{N}$ finite and $0 \in A$

- 1: $B = \{0\}$, $N = \max A$
- 2: **while** $(A + B)_{0-p} \neq \overline{1}^n$ for some n **do**
- 3: $i \leftarrow$ first index such that $(A + B)_{0-p} \neq 1 \bmod p$
- 4: **if** $i \neq (\max B + \max A + 1)$ **then**
- 5: $B := B \cup \{i\}$
- 6: $N := i + \max A$
- 7: **else**
- 8: break while


```

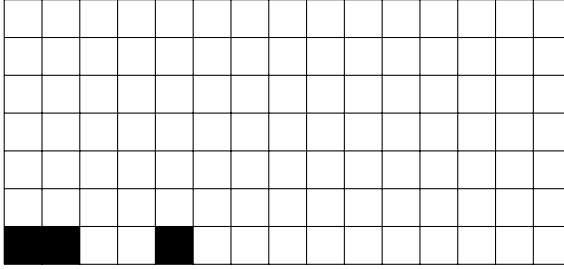
9:   end if
10: end while
11: return  $(B, N)$ 

```

Example 2.21 This algorithm is really easy to understand from a graphical point of view. Indeed, if one considers the representation in a grid, it means adding the rhythmic pattern A at the earliest time when there is not 1 mod p onset. It is also a good way to understand the notions of definitions 2.11 and 2.15.

See the algorithm applied to $A = \{0, 1, 4\}$. For better understanding, at every step depicted of the algorithm, we will show the value of $(A + B)_{0-2}$ and of the smaller uner-cover $UC_2(i)$ the algorithm is trying to fill.

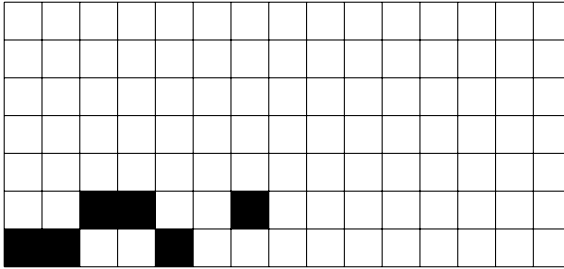
Step 1:



$$(A + B)_{0-2} = 11001000 \dots$$

$$UC_2(2) = 001$$

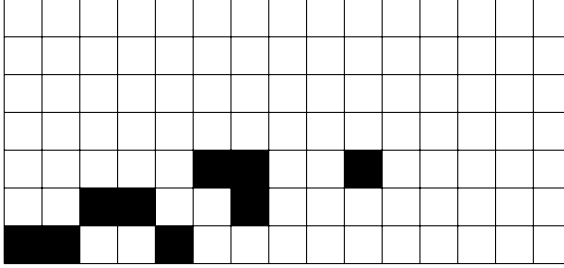
Loop while with $i = 2$:



$$(A + B)_{0-2} = 1111101$$

$$UC_2(5) = 01$$

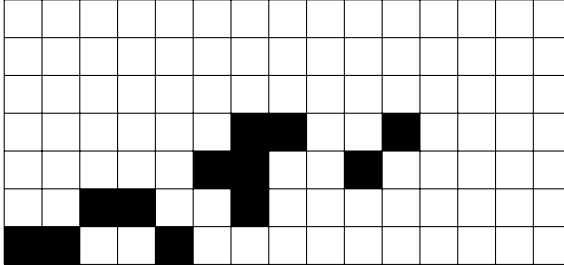
With $i = 5$:



$$(A + B)_{0-2} = 1111110001$$

$$UC_2(6) = 0001$$

With $i = 6$:

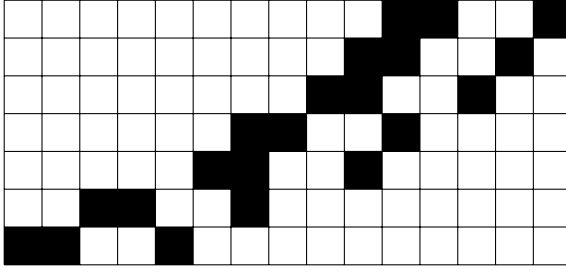


$$(A + B)_{0-2} = 11111111011$$

$$UC_2(8) = 011$$

\vdots

With $i = 10$:



$$(A+B)_{0-2} = 111111111111111$$

$$UC_2(15) = \text{empty word}$$

The next step gives $i = 15 = \max B + \max A + 1$.

Remark 2.22 Such a tiling is not unique: the rhythmic pattern $A = \{0, 1, 4\}$ tiles with $B = \{0, 2, 5, 6, 8, 9, 10\}$, but also with the following B_i :

- $B_1 = \{0, 2, 5, 6, 8, 9, 10, 15, 17, 20, 21, 23, 24, 25\}$
- $B_2 = \{0, 2, 5, 6, 8, 9, 10, 15, 17, 20, 21, 23, 24, 25, 30, 32, 35, 36, 38, 39, 40\}$
- ...

PROPOSITION 2.23 *This greedy algorithm is optimal in the sense that it gives the smallest number of entries $\sharp B$ (and so the smallest N) such that (A, B) is a compact RT_pC of \mathbb{Z}_N .*

Proof. Let p be a prime number, and A a rhythmic pattern such that it admits a compact RT_pC . *Reductio ad absurdum*, let us suppose there exists \tilde{B} such that (A, \tilde{B}) is a compact RT_pC of $\mathbb{Z}_{\tilde{N}}$ and $\sharp \tilde{B} < \sharp B$ with B the output of the algorithm.

$\tilde{B} \not\subseteq B$ because since (A, \tilde{B}) is a compact RT_pC , it means that during the algorithm, the smallest element i of $B \setminus \tilde{B}$ would verify line 4: $i = \max \tilde{B} + \max A + 1$ and hence $B = \tilde{B}$.

We can suppose without loss of generality that B and \tilde{B} are sorted. Let i the smallest index such that $\tilde{B}[i] = \tilde{b} < B[i] = b$.

After $i - 1$ loops, the algorithm produces the subset $B[0, \dots, i - 1]$ providing the same under-cover $UC_p(0)$ as the subset $\tilde{B}[0, \dots, i - 1]$:

$$UC_p(0) = (A+B[0, \dots, i-1])_{0-p}[0, \dots, N-1] = (A+\tilde{B}[0, \dots, i-1])_{0-p}[0, \dots, N-1].$$

Since \tilde{B} tiles with A , at time \tilde{b} , there cannot be exactly 1 mod p onset in the under-cover: $UC_p(0)[\tilde{b}] \neq 1 \pmod{p}$. Step 3 of the algorithm, during the i -th loop, returns the smallest index b' such that at this index of the under-cover there is anything but 1 mod p onset, and will give a $b' \leq \tilde{b} < b$, which is a contradiction with the fact that the i -th element of B is b . ■

Example 2.24 As we can see in example 2.21, the smallest number of entries to tile modulo 2 with $A = \{0, 1, 4\}$ is 7.

Remark 2.25 Thanks to theorem 1.15, we have seen that VC are the basis of RTC under the concatenation operation. Also, corollary 1.23 gives us the result that VC are the key to attaining a necessary and sufficient condition on the tiling property of a rhythmic pattern.

This greedy algorithm provides minimal RT_pC under concatenation. They are the “modulo p Vuza canons”. We hope that a connection can be established between both kinds of Vuza canons, the latter modulo p being relatively easy to compute, to be able

to return to classical VC and thus obtain a faster way to enumerate them. It remains, however, a distant ambition. There are two principal differences between classical VC and the RT_pC ones we are working with. First, the algorithm only computes compact RT_pC , whereas VC are not usually compact. Future research, with the aim of linking back those two types of canons, will have to search and compute minimal non compact mod p Vuza canons, i.e. minimal under concatenation and duality, but also tiling a smaller period than the compact one. The second difference is of course the distinction between tiling \mathbb{Z} and tiling \mathbb{F}_p . A VC admits one and only one onset every beat, unlike RT_pC s which admit one modulo p per beat. So we need to understand how to remove those extra onsets. The paper will now focus on a better understanding of this latter challenge.

The goal is to understand when and how we are able to obtain ‘*donsets*’, a neologism introduced here to express the fact that the onsets have copies at this time, giving us a covering instead of a tiling. This term is also a contraction of *d*-onset, and if we have 3 layered notes, we can talk about a 3-onset.

DEFINITION 2.26 *We note the multiset of donsets of the $RT_pC(A, B)$ of \mathbb{Z}_N :*

$$D_{(A,B),p} = \bigcup_{n \in \mathbb{Z}_N} \bigcup_{\substack{kp, \\ k \in \mathbb{N}^*, \\ \mathbb{1}_{(A+_NB)}(n)=kp+1}} \{n\}$$

One can extend the notion of duality to compact RT_pC :

PROPOSITION 2.27 *(A, B) is a (resp. compact) RT_pC iff (B, A) is a (resp. compact) RT_pC and $D_{(A,B),p} = D_{(B,A),p}$.*

Proof. Let (A, B) be a (resp. compact) RT_pC of \mathbb{Z}_N . $C = A +_N B$ (resp. $C = A + B$) is a multiset such that:

$$C = \left\{ \underbrace{0, 0, \dots, 0}_{k_0p+1 \text{ times}}, \underbrace{1, 1, \dots, 1}_{k_1p+1 \text{ times}}, \dots, \underbrace{N-1, N-1, \dots, N-1}_{k_{N-1}p+1 \text{ times}} \right\}$$

with $\forall i \in \llbracket 0, N-1 \rrbracket$, $k_i \in \mathbb{N}$.

By commutativity in \mathbb{Z} , we get that $C = B +_N A$ (resp. $C = B + A$), hence (B, A) is a (resp. compact) RTC of \mathbb{Z}_N modulo p , and the donsets correspond to the $k_i \neq 0$ and are at the same positions $a + b \bmod N = b + a \bmod N$ (resp. $a + b = b + a$) and in the same amount $k_i p$. ■

Remark 2.28 However, if B is the smallest rhythmic pattern obtained by the algorithm for a given A , A may not be the smallest complement obtained by the algorithm if the entry is B , if A is a concatenation of different rhythmic patterns that tile with B .

For instance, if the rhythmic pattern in entry is $A = \{0, 1, 2, 6, 7, 8\}$, the algorithm modulo 2 returns $B = \{0, 3\}$ for which it returns $A' = \{0, 1, 2\}$. In such cases, we always have that such an A' is always a subset of A .

Remark 2.29 If the tiling is not compact, the best way we currently have to compute the size of a RTC quickly is the algorithm presented in (Amiot 2011) which returns a multiple of the size of the smallest RTC with a given rhythmic pattern; this is achieved by incrementing the suitable values of N until we can find one such that $A(X)$ divides $X^N - 1$ modulo p . One must bear in mind that in order to discover the exact size of the

n	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
N	3	7	15	21	63	127	63	73	889	1533	3255	7905	11811	32767	255

Table 1.: Size N of the minimal compact RT_2C with the rhythmic pattern $A = \{0, 1, n\}$.

smallest RTC, one needs the greedy algorithm when the tiling is compact.

See, in Table 1 the minimal size of RT_2C (hence compact) of rhythmic pattern $A = \{0, 1, n\}$ for some small n obtained with the greedy algorithm.

One can notice that rhythmic patterns of the form $A_k = \{0, 1, 2^k\}$ give smaller compact RTC. We will now focus on these patterns.

3. The case $A_k = \{0, 1, 2^k\}$

The following theorem is the main new result of this paper, and is the first cardinality result for RT_pC .

THEOREM 3.1 *For all $k \in \mathbb{N}^*$, the rhythmic patterns couple $(A_k, B_k) = (\{0, 1, 2^k\}, B_k)$ is the smallest compact RT_2C of \mathbb{Z}_N , and is of size $N = 4^k - 1$ with $\sharp B_k = 4^k - 3^k$ entries, and $\sharp D_{(A_k, B_k), 2} = 4^k - \frac{3^{k+1} - 1}{2}$ donsets.*

Thanks to a constructive proof, this theorem allows us to build the pattern of entries B_k which tiles modulo 2 with a given $A_k = \{0, 1, 2^k\}$. Since one can also easily prove that in this case one cannot have d -onsets with $d > 3$, one arrives at a comprehensive enumeration: the number of entries, the size of the RTC, and the number of donsets.

Before giving a formal proof, we will start with an explanation of how those tilings are built, which will in turn demonstrate the general concept of the proof. Some technical lemmas will form the second part of this proof, and we will finish with the formal demonstration of the theorem.

3.1. Introduction

Let us begin with a close look at how the greedy algorithm builds a tiling with the pattern $A_3 = \{0, 1, 8\}$.

At step 1, the algorithm places the pattern A_3 at the first position, that is to say $B = \{0\}$, hence $(A + B)_{0-2} = 110000001$.

The algorithm then enters the **while** loop, and tries first to fill the under-cover $UC_2(2) = 0000001$. It is filled with the entries $B' = \{0, 2, 4\}$ which gives after three steps 3 of the algorithm $B = B \cup (\{0, 2, 4\} + \{2\}) = \{0, 2, 4, 6\}$, thus $(A + B)_{0-2} = 11111111010101$. The algorithm goes again in the while loop, trying now to fill the under-cover $UC_2(9) = 010101$. And so on.

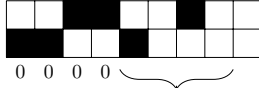
The idea is to fill the current under-cover, and doing so, we get a new under-cover: the “following under-cover” of definition 2.15 ; and we keep on filling it until we obtain a compact tiling, that is to say an empty or null under-cover. The entries pattern B_k is built in this incremental way, filling the following under-covers one after another during the **while** loop.

Remark 3.2 Let $i \in \mathbb{N}$, our rhythmic pattern $A_k = \{0, 1, 2^k\}$ being of size $\max(A_k) - \min(A_k) = 2^k$, if, to fill any under-cover of size 2^k starting at index i (and ending at index $i + 2^k - 1$) we need the entries B' , then the following under-cover of size 2^k (and

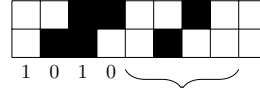
you can find one of this size) and starting at index $i + 2^k$ will be B'_{0-1} . This fact is due to the gap between the first onsets $\{0, 1\}$ and the third and last onset $\{2^k\}$ of A_k .

Example 3.3 Let $A_2 = \{0, 1, 4\}$ and $B = \{0, 2\}$ which fills the null under-cover 0000 starting at index 0. We then obtain $(A_2 + B)_{0-2} = 1111010$, hence the following under-cover starting at index $2^2 + 0 = 4$ and of size 4 is $1010 = B_{0-1}$.

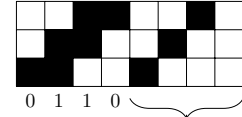
$$A + B, B_{0-1} = 1010$$



$$A + B', B'_{0-1} = 0110$$



$$A + B'', B''_{0-1} = 1110$$



An efficient way to exploit this phenomenon is to build B_k in a recursive way. If we write $(B_k)_{0-1}$ in an array $V(k)$ with 2^k columns, from left to right then top to bottom, we obtain that every line ℓ of $V(k)$ is the following under-cover of the under-cover obtained with A_k and $(B_k)_{0-1}$ read in lines $1 \dots \ell - 1$.

Example 3.4 For a better understanding, here are A_k , B_k , $(B_k)_{0-1}$ and $(B_k)_{0-1}$ in the $V(k)$ array for $k = 1, 2, 3$:

- $k = 1, A_1 = \{0, 1, 2\}, B_1 = \{0\}, (B_1)_{0-1} = 1$
 $V(1) = (10)$
- $k = 2, A_2 = \{0, 1, 4\}, B_2 = \{0, 2, 5, 6, 8, 9, 10\},$
 $(B_2)_{0-1} = 10100110111$
 $V(2) = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 \end{pmatrix}$
- $k = 3, A_3 = \{0, 1, 8\},$

$$B_3 = \{0, 2, 4, 6, 9, 10, 13, 14, 16, 17, 18, 20, 21, 22, 27, 28, 29, 30, 32, \\ 34, 35, 36, 37, 38, 41, 42, 43, 44, 45, 46, 48, 49, 50, 51, 52, 53, 54\}$$

$$(B_3)_{0-1} = 101010100110011011101110000111101011111001111101111110$$

$$V(3) = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \end{pmatrix}$$

DEFINITION 3.5 Let $k \in \mathbb{N}^*$, B a pattern, and UC_2 an under-cover of (A_k, B) of size $n \leq 2^k$. We denote \xrightarrow{k} a postfix function over and to the finite words over the alphabet $\{0, 1\}$ defined by $UC_2 \xrightarrow{k} (B')_{0-1}$ iff the pattern B' of size n (you can pad in some 0s in the end to adjust the size) fills UC_2 with A_k .

Example 3.6 We have $\overline{0}^{2n} \xrightarrow{k} \overline{10}^n$ if $2n \leq 2^k$.

See in example 3.4 above, for $k = 3$ and $n = 4$, one can see that the following under-

cover of $\bar{0}^8$ of size 8 (which is the first under-cover of the tiling) is $\bar{10}^4$.

Remark 3.7 Thanks to remark 3.2, we know that the pattern B_k such that (A_k, B_k) is a RT_2C can be written in the form $(B_k)_{0-1} = \tilde{B}_1 \cdots \tilde{B}_n$ with

$$\forall i \leq n \ |\tilde{B}_i| = 2^k \text{ and } \bar{0}^{2^k} \xrightarrow{k} \tilde{B}_1 \xrightarrow{k} \dots \xrightarrow{k} \tilde{B}_n$$

and the theorem's proof will yield $n = 2^k - 1$. It means that every under-cover \tilde{B}_i will be the following under-cover of the under-cover \tilde{B}_{i-1} as defined in 2.15.

Written in the array $V(k)$ as defined earlier, it means that $V(k) = \begin{pmatrix} \tilde{B}_1 \\ \tilde{B}_2 \\ \dots \\ \tilde{B}_n \end{pmatrix}$.

Example 3.8 With $k = 2$, we have $\bar{0}^4 \xrightarrow{2} 1010 \xrightarrow{2} 0110 \xrightarrow{2} 1110$ and indeed we have $(B_2)_{0-1} = 10100110111 = 101001101110$ that is to say:

$$V(2) = \begin{pmatrix} 1010 \\ 0110 \\ 1110 \end{pmatrix}.$$

DEFINITION 3.9 Let us define the array $T(k)$ by induction over $k \in \mathbb{N}^*$:

Let $T(1) = (10)$. If one has the array $T(k)$ of size $(2^k - 1, 2^k)$, one can build the array $T(k+1)$ of size $(2^{k+1} - 1, 2^{k+1})$ in this way:

$$\left(\begin{array}{c|c} T(k) & T(k) \\ \hline & 11 \dots 1 0 \\ & 11 \dots 1 0 \\ \widetilde{T(k)} & \vdots \quad \vdots \\ & 11 \dots 1 0 \end{array} \right)$$

with $\widetilde{T(k)}$ being an array of size $(2^k, 2^k)$ defined by: its first line is $\bar{0}^{(2^k-1)}1$, and its last lines are $T(k)$ whose last column of 0 is changed into a column of 1 (one can easily prove by construction that the last column of $T(k)$ is null for all k).

Example 3.10 See for some values of k the array $T(k)$ with separation lines from the inductive construction:

$$T(1) = (10)$$

$$T(2) = \left(\begin{array}{c|c} 10 & 10 \\ \hline 01 & 10 \\ 11 & 10 \end{array} \right)$$

$$T(3) = \left(\begin{array}{c|c} 1010 & 1010 \\ \hline 0110 & 0110 \\ 1110 & 1110 \\ \hline 0001 & 1110 \\ 1011 & 1110 \\ 0111 & 1110 \\ 1111 & 1110 \end{array} \right)$$

$$\text{where we can see } \widetilde{T(2)} = \begin{pmatrix} 0001 \\ 1011 \\ 0111 \\ 1111 \end{pmatrix}$$

Remark 3.11 The proof of the theorem will be to establish the equality $V(k) = T(k)$ for all $k \in \mathbb{N}^*$. For this purpose we need some technical lemmas presented in the next part of this proof.

3.2. Lemmas

LEMMA 3.12 For all $n \in \mathbb{N}^*$, to fill an under-cover $UC_2(i)_n = 0\bar{1}^n 0$ starting at index i with the pattern 11, one needs the entries $B'_{0-1} = \bar{1}^{n+1} 0$.

Proof. By induction over n .

If $n = 1$, to fill the under-cover $UC_2(i)_1 = 010$ with the pattern 11, one needs to put an onset at index i , hence $B'_{0-1} = 1 \dots$. The new under-cover is $100 = 1(1 + 1 \bmod 2)0$. One then needs to put the pattern at index $i + 1$ to fill the new 0, hence $B'_{0-1} = 11 \dots$. The new under-cover being 111, the under-cover is a tiling and we do not need any more entry, hence $B'_{0-1} = 110$.

Assume the lemma is true for some n , let us see how one can fill the under-cover $UC_2(i)_{n+1} = 0\bar{1}^{n+1} 0$ starting at index i with the pattern 11.

The under-cover starts with a 0, hence the word of the filling pattern starts with a 1, i.e. $B'_{0-1} = 1 \dots^{n+2}$, and the new under-cover is $10\bar{1}^n 0 = 1(1 + 1 \bmod 2)\bar{1}^n 0 = 1 \cdot UC_2(i+1)_n$. By induction hypothesis, to tile the $n + 2$ last index of this under-cover, the $n + 2$ last terms of the entries B'_{0-1} have to be $\bar{1}^{n+1} 0$. Hence we have $B'_{0-1} = 1\bar{1}^{n+1} 0 = \bar{1}^{n+2} 0$. ■

LEMMA 3.13 $\forall k \in \mathbb{N}, \bar{1}^{(2^k-1)} 0 \bar{1}^{(2^k-1)} 0 \xrightarrow{k+1} \bar{0}^{(2^k-1)} 1 \bar{1}^{(2^k-1)} 0$

Proof. Let us denote $\bar{1}^{(2^k-1)} 0 \bar{1}^{(2^k-1)} 0 \xrightarrow{k+1} \tilde{C}$.

The first block of 1s of size $2^k - 1$ is already a tile, there is no need of entries for those $2^k - 1$ first indexes, hence the word \tilde{C} starts with $\bar{0}^{2^k-1}$.

We then arrive to the second block $0 \bar{1}^{(2^k-1)} 0$, whose length verifies $|0 \bar{1}^{(2^k-1)} 0| < 2^{k+1}$. Only the first two onsets of $A_{k+1} = \{0, 1, 2^{k+1}\}$ are used to tile the under-cover, hence we try to tile the rest of \tilde{C} with the pattern $\{0, 1\}_{0-1} = 11$. So the filling verifies the conditions of lemma 3.12, meaning $\tilde{C} [2^k \dots 2^{k+1}] = \bar{1}^{2^k} 0$.

We indeed have $\tilde{C} = \bar{0}^{(2^k-1)} 1 \bar{1}^{(2^k-1)} 0$. ■

LEMMA 3.14 $\forall k \in \mathbb{N}^*, \forall n < 2^k - 2, 0\bar{1}^n 0 \xrightarrow{k} \bar{1}^{(n+1)} 0$.

Proof. Since $|0\bar{1}^n 0| < 2^k$, we only tile with the first two onsets 11 of the pattern A_k , and we are again in the conditions of lemma 3.12. ■

LEMMA 3.15 $\forall k \in \mathbb{N}, 0\bar{1}^{(2^k-2)} 0 \xrightarrow{k} \bar{1}^{(2^k)}$

Proof. In this case, we don't have $|0\bar{1}^{(2^k-2)} 0| < 2^k$ and we cannot use lemma 3.12. However, we have exactly $|0\bar{1}^{(2^k-2)} 0| = 2^k$. It means that we are out of lemma 3.12 conditions only for the last index. Hence if we have to add a pattern at the first index (and since the under-cover $0\bar{1}^{(2^k-2)} 0$ starts with a 0 we will have to), we can consider the same under-cover with an additional onset at its last index $0\bar{1}^{(2^k-2)} 1$ that we tile with the pattern 11.

By an induction like the one used to prove lemma 3.12, we obtain the entries $\bar{1}^{(2^k-1)} 0$.

But the 0 on the last index is already filled by the last onset of A_k , so we only need to add a last time the pattern A_k at the last index, and the following under-cover is $\bar{1}^{(2^k)}$. ■

LEMMA 3.16 $\forall k \in \mathbb{N}$, if $|A| = |B| = 2^k - 1$, if $A \cdot 0 \xrightarrow{k} B \cdot 0$ then $A \cdot 1 \xrightarrow{k} B \cdot 1$, with $U \cdot u$ being the concatenation of the word U to the letter u .

Proof. By definition of an under-cover, adding some zeros at the end does not change it, so $A = A \cdot 0$. If we denote \tilde{B} (resp. $\tilde{B}1$) the rhythmic pattern such that $A = A \cdot 0$ (resp. $A \cdot 1$) is the $UC_2(i)$ of (A_k, \tilde{B}) (resp. of $(A_k, \tilde{B}1)$), and associate the words A, B with the sets A, B we have by definition

$$\left(A_k + \left(\tilde{B} \cup (B + \{i\}) \right) \right)_{0-2} [0, \dots, i + 2^k - 1] = \bar{1}^i \bar{1}^{|A \cdot 0|} \text{ and } (A_k + \tilde{B})_{0-2} = \bar{1}^i \cdot A \cdot 0.$$

Denoting by C a multiset of the form

$$C = \left\{ \underbrace{0, 0, \dots, 0}_{2k_0+1 \text{ times}}, \underbrace{1, 1, \dots, 1}_{2k_1+1 \text{ times}}, \dots, \underbrace{i-1, i-1, \dots, i-1}_{2k_{i-1}+1 \text{ times}} \right\}$$

with $\forall n \in [0, i-1]$, $k_n \in \mathbb{N}$ such that $A_k + \tilde{B} = C \cup (A + \{i\})$, we have

$$([C \cup (A + \{i\})] \cup [A_k + (B + \{i\})])_{0-2} [0, \dots, i + 2^k - 1] = \bar{1}^i \bar{1}^{|A \cdot 0|}$$

or, since $|B| = 2^k - 1$,

$$(C \cup (A + \{i\}) \cup (\{0, 1\} + (B + \{i\})))_{0-2} [0, \dots, i + 2^k - 1] = \bar{1}^i \bar{1}^{|A \cdot 0|}$$

by removing the i -th first indexes of $\bar{1}^i \bar{1}^{|A \cdot 0|}$ that come from C

$$((A + \{i\}) \cup (\{0, 1\} + (B + \{i\})))_{0-2} [0, \dots, i + 2^k - 1] = \bar{0}^i \bar{1}^{|A \cdot 0|}$$

so, by excising the i -th first beats:

$$(A \cup (\{0, 1\} + B))_{0-2} [0, \dots, 2^k - 1] = \bar{1}^{|A \cdot 0|} = \bar{1}^{2^k}$$

When one fills the under-cover $A \cdot 0$, one needs the entries $B \cdot 0$. Likewise, since the sets associated with the words $A \cdot 0$, $B \cdot 0$ are the same as those associated with the words A, B by definition, we have, using the same notation

$$(A \cdot 0 \cup (\{0, 1\} + B \cdot 0))_{0-2} [0, \dots, 2^k - 1] = \bar{1}^{|A|+1}$$

The sets $A \cdot 1$, $B \cdot 1$ associated with the words $A \cdot 1$, $B \cdot 1$ verify $A \cdot 1 = A \cup \{2^k\}$, $B \cdot 1 = B \cup \{2^k\}$.

We have

$$\begin{aligned}
(A \cdot 1 \cup (\{0, 1\} + B \cdot 1)) &= ((A \cup \{2^k\}) \cup (\{0, 1\} + (B \cup \{2^k\}))) \\
&= (\{2^k\} \cup A \cup (\{0, 1\} + B) \cup (\{2^k, 2^k + 1\})) \\
&= ((A \cup (\{0, 1\} + B)) \cup (\{2^k, 2^k + 1\}))
\end{aligned}$$

Thus

$$(A \cdot 1 \cup (\{0, 1\} + B \cdot 1))_{0-2} = \bar{1}^{2^k-1}(1+1+1)1 = \bar{1}^{|A|+1}$$

So, by adding the first i beats with a multiset $C1$ such that $A_k + \tilde{B}1 = C1 \cup (A \cdot 1 + \{i\})$, we have

$$([C1 \cup (A \cdot 1 + \{i\})] \cup [A_k + (B \cdot 1 + \{i\})])_{0-2} [0, \dots, i + 2^k - 1] = \bar{1}^i \bar{1}^{|A \cdot 1|}$$

which means

$$(A_k + (\tilde{B}1 \cup (B \cdot 1 + \{i\})))_{0-2} [0, \dots, i + 2^k - 1] = \bar{1}^i \bar{1}^{|A \cdot 1|},$$

we indeed have that $A \cdot 1 \xrightarrow{k} B \cdot 1$. ■

LEMMA 3.17 $\forall n, k \in \mathbb{N}, \forall a \in \{0, 1\}$, if $|A| = |B| = 2^k - 1$, if $A \cdot a \xrightarrow{k} B \cdot 0$ then $\overline{A \cdot a}^n \xrightarrow{k+n-1} \overline{B \cdot 0}^n$.

Proof. The fact that $B \cdot 0$ ends with a 0 means that to fill $A \cdot a = UC_2(i)$, one does not need to put the pattern 11 (first two onsets of A_k) at index $i + 2^k$. Hence we do not brim over the 2^k -sized following under-cover when filling $A \cdot a$ with B . To fill the following under-cover we do not need to keep the memory of the previous filling (except for the last onset of A_k which creates the following under-cover of course). We can concatenate the filling pattern if we want to fill the n -concatenation of the under-cover, taking care to tile with $\{0, 1, 2^{k+n-1}\}$ instead of $\{0, 1, 2^k\}$ to make sure that we will not run into the last onset of A_{k+n-1} and that we will only use the first two onsets 11 during the filling. ■

Those previous lemmas help for the recursive proof of the equality $V(k) = T(k)$, whereas the next one will be used for the cardinality result.

LEMMA 3.18 If one constructs a minimal RT_2C with A such that $\sharp A = n$, then every k -onset verifies $k \leq n$.

Proof. Let $A = \{a_1, \dots, a_n\}$, B such that (A, B) is a RT_2C of \mathbb{Z}_N and suppose a k -onset at time t with $k > n$.

This k -onset is built from different layered onsets of A : a_{j_1}, \dots, a_{j_k} , and we note b_{j_i} the voice entry in B that produces the onset a_{j_i} played at time t .

Since $k > n$, by the pigeonhole principle, there exists $j_i \neq j_l$ such that $a_{j_i} = a_{j_l}$. Hence the rhythmic pattern is played twice at the same entry $b_{j_i} = b_{j_l} = t - a_{j_i}$. So, at every

time $b_{j_i} + a_m = b_{j_i} + a_m$, $m = 1, \dots, k$, there is two onsets layered from A , that counts as 0 mod 2.

So, if we will have the exact same number of onsets mod 2 at every time of $A +_N B$ and $A +_N (B \setminus \{b_{j_i}, b_{j_i}\})$.

Hence $(A, B \setminus \{b_{j_i}, b_{j_i}\})$ is a smaller RT_2C of \mathbb{Z}_N , which is a contradiction with the fact that (A, B) is minimal. ■

3.3. Proof of the Theorem

To prove theorem 3.1, we will start to prove the

THEOREM 3.19 *The array $T(k)$ built previously in definition 3.9 is equal to the array*

$$V(k) = \begin{pmatrix} \tilde{B}_1 \\ \tilde{B}_2 \\ \dots \\ \tilde{B}_n \end{pmatrix}$$

with $B_k = \tilde{B}_1 \dots \tilde{B}_n$, i.e. $\bar{0}^{2^k} \xrightarrow{k} \tilde{B}_1 \xrightarrow{k} \dots \xrightarrow{k} \tilde{B}_n$ and $|\tilde{B}_i| = 2^k$.

Proof. Let us prove this equality by induction over k :

If $k = 1$, we have indeed $T(1) = (10) = V(1)$ and the pattern of entries is $B_1 = \{0\}$.

If the equality is true for some k , let us prove it for $k + 1$:

By lemma 3.17 with $n = 2$ we obtain that if $T(k)$ gives the pattern of entries to tile with the pattern A_k , then $(T(k)|T(k))$ gives the beginning of the pattern of entries to tile with A_{k+1} . Indeed, we proceed by blocks of size 2^{k+1} before we come to the last onset of A_{k+1} .

By lemma 3.13, we obtain the construction of the first line of the bottom block of $T(k + 1)$, i.e. the first line of $\widetilde{T(k)}$ which is $\bar{0}^{(2^k-1)}1$ adjoined to $\bar{1}^{2^k-1}0$.

By lemma 3.14, we obtain the block at the bottom-right of $T(k + 1)$:

$$\begin{array}{l} 11 \dots 10 \\ 11 \dots 10 \\ \vdots \\ 11 \dots 10 \end{array}$$

Indeed, one can notice that we always have a 0 before those lines of 1s, so we are in the condition of lemma 3.14; if we didn't, it means that we have a line full of 1s, and hence we are in the case of lemma 3.13 which entails having a complete tiling with A_{k+1} and finishing the equality, see later when we use lemma 3.15 (or going towards step $k + 2$).

Lemma 3.16 explains why all but the first lines of $\widetilde{T(k)}$ look like $T(k)$. We try to tile with the pattern 11, since the last onset of A_{k+1} is not taken into account in a block of such size. With the recursion hypothesis $V(k) = T(k)$, the procedure gave us the word in $T(k)$, and we can think of it as though we were filling a previous line of 0s, as it is highlighted in remark 2.14. Here the previous line is $\bar{0}^{2^k-1}1$, the first line of $\widetilde{T(k)}$, hence the following word obtained is $T(k)$ but with a 1 instead of a 0 in its last column as shown in lemma 3.16.

Finally, lemma 3.15 proves the end of construction. The last line of $T(k+1)$ is $\overline{1}^{(2^{k+1}-1)}$ which gives a tiling modulo 2 with $A_{k+1} = \{0, 1, 2^{k+1}\}$ because we use in last position (index 2^{k+1} of this line) the last onset of A_{k+1} . Indeed this sequence of $2^{k+1}-1$ consecutive entries gives a tiling modulo 2 which is followed by $2^{k+1}-1$ onsets not donsets, finishing the tiling.

We can now conclude by induction that $\forall k \in \mathbb{N}^*$ the array $T(k)$ built like in definition 3.9 is equal to $V(k)$, i.e. is the array containing $(B_k)_{0-1}$ written line by line. ■

Now that we have proved this first result, we know how to construct the pattern of entries B_k , and in order to obtain the cardinality results in theorem 3.1, we just have to tally in $T(k)$.

Proof. The number of entries $b(k) = \sharp B_k$ is the number of 1s in the array $T(k)$ and we can count them by induction:

We have $b(1) = 1; b(2) = 7$.

By construction of $T(k+1)$, we have the equality

$$b(k+1) = 3 \times b(k) + 4^k.$$

Indeed, the term $3 \times b(k)$ comes from the array $T(k)$ put three times in $T(k+1)$ and the term 4^k is from the bottom right block of 1s of size $(2^k, 2^k)$.

One can verify easily that for all k , $b(k+2) - 7b(k+1) + 12b(k) = 0$, hence

$$b(k) = \frac{b(2) - 3b(1)}{4} \times 4^k - \frac{4b(1) - b(2)}{3} \times 3^4 = 4^k - 3^k.$$

To obtain the size N of the RTC, we know that it will end with putting the pattern A_k on the last 1 of $(B_k)_{0-1}$, so

$$N = (2^k - 1) \times 2^k - 1 + 2^k = 4^k - 1.$$

The first product comes from the size $(2^k, 2^k - 1)$ of the array $T(k)$, and the next -1 from the fact that the last 1 in $T(k)$ is on the penultimate position. The last $+2^k$ is from the addition of the pattern A_k at this index.

Finally, to enumerate the donsets, we simply use lemma 3.18. In our case, we have $\sharp A_k = 3$, so donsets cannot have more than 3 onsets layered. And since we obtain a RT_2C , it means that there is 1 or 3 onsets at each time, so every donset is a 3-onset.

Hence, if we note D_k the set of index where there is a donset, we have the formula

$$\sharp A_k \times \sharp B_k - 2\sharp D_k = N.$$

Indeed the factor 2 multiplying $\sharp D_k$ comes from this lemma 3.18, saying that every donset is exactly two onsets above a classical tiling; the result follows: $\sharp D_k = \frac{4^k - 3^{k+1} - 1}{2}$. ■

4. Conclusion

Finding a way to obtain all the VC of a given period \mathbb{Z}_N is an issue for composers. It is also a major challenge for mathematicians, as solving the Coven-Meyerowitz conjecture could help to solve the spectral conjecture in dimension 1. This conjecture, also called the Fuglede conjecture, has recently been proved to be false for dimensions higher or equal to 5 (Tao 2003), and from this work, Matolcsi (2005) has proved it to be false in dimensions 3 and 4. The problem remains open in smaller dimensions.

During the last decade, many approaches have been tested to built and understand VC: exhaustively (Kolountzakis and Matolcsi 2009), by using perturbations of periodic tilings (Kolountzakis et al. 2003), through transformations that conserve the property of being a VC (Amiot 2005)...

This article introduces a new approach with the modulo p VC, and especially modulo 2, which are substantially easier to compute. It is also a sub-problem of a cryptographic issue: factorisation of polynomials in $\mathbb{F}_2[X]$, which is equivalent to the factorisation of some multisets. The interested reader can find a recent work on factorisation of a multiset into two multisets (Neumann and Praeger 2004). The modulo p VC problem can be rephrased as the still unresolved mathematical topic of factorisation of a multiset into two proper sets: a new mathematical branch to explore, rising from a musical bough.

References

- Amiot, Emmanuel. 2004. "Why rhythmic Canons are interesting." *E. Lluís-Puebla, G. Mazzola et T. Noll (eds.), Perspectives of Mathematical and Computer-Aided Music Theory, EpOs* 190–209.
- Amiot, Emmanuel. 2005. "Rhythmic canons and Galois theory." *Colloquium on mathematical music theory, H. Friepertinger (ed.)*.
- Amiot, Emmanuel. 2011. "Structures, Algorithms and algebraic tools for rythmic canons." *Perspectives of New Music* 49 (2): 93–142.
- Andreatta, Moreno. 1996. "Gruppi di Hajós, Canoni e Composizioni." Master's thesis. Tesi di Laurea, Facoltà di Matematica dell'Università degli Studi di Pavia.
- Andreatta, Moreno, and Carlos Agon, eds. 2009. *Journal of Mathematics and music, Special issue: Tiling Problems in Music*. Vol. 3,2. Taylor and Francis.
- Boretz, Benjamin, Robert Morris, and John Rahn, eds. 2011. *Perspectives of New Music, Special issue: Perspectives on Tiling Rhythmic Canons*. Vol. 49,2. Perspectives of New Music.
- Coven, Ethan M, and Aaron Meyerowitz. 1999. "Tiling the integers with translates of one finite set." *Journal of Algebra* 212 (1): 161–174.
- De Bruijn, Nicolaas Govert. 1953. "On the factorization of cyclic groups." *Indag. Math* 15: 370–377.
- Hajós, György. 1949. "Sur la factorisation des groupes abéliens." *Časopis Pest. Mat. Fys* 74: 157–162.
- Kolountzakis, Mihail N, et al. 2003. "Translational tilings of the integers with long periods." *Journal of Combinatorics* 10.
- Kolountzakis, Mihail N, and Máté Matolcsi. 2009. "Algorithms for translational tiling." *Journal of Mathematics and Music* 3 (2): 85–97.
- Lagarias, Jeffrey C, and Yang Wang. 1996. "Tiling the line with translates of one tile." *Inventiones mathematicae* 124: 341–365.
- Matolcsi, Máté. 2005. "Fuglede's conjecture fails in dimension 4." *Proceedings of the American Mathematical Society* 133 (10): 3021–3026.
- Neumann, Peter M, and Cheryl E Praeger. 2004. "On Tensor-Factorisation Problems, I: The Combinatorial Problem." *LMS J. Comput. Math* 7: 73–100.
- Rédei, László. 1950. "Ein Beitrag zum Problem der Faktorisierung von endlichen Abelschen Gruppen." *Acta Mathematica Hungarica* 1 (2): 197–207.
- Sands, Arthur D. 1957. "On the factorisation of finite abelian groups." *Acta Mathematica Hungarica* 8 (1): 65–86.
- Tao, Terence. 2003. "Fuglede's conjecture is false in 5 and higher dimensions." *arXiv preprint math/0306134*.
- Vuza, Dan Tudor. 1985. "Sur le rythme périodique." *Revue Roumaine de Linguistique-Cahiers de Linguistique Théorique et Appliquée* 22 (1): 173–188.

- Vuza, Dan Tudor. 1991-1993. "Supplementary sets and regular complementary unending canons." *Perspectives of New Music* In four parts.
- Warusfel, André. 1971. *Structures algébriques finies: groupes, anneaux, corps*. Vol. 10. Hachette.